TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 1511	**POUR SUITE À DONNER** voir le formulaire PCT/ISA/220 et, le cas échéant, le point 5 ci-après.	
Demande internationale n° PCT/EP2004/051144	Date du dépôt international *(jour/mois/année)* 17/06/2004	(Date de priorité (la plus ancienne) *(jour/mois/année)* 18/06/2003
Déposant GEMPLUS		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 6 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**
   a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous ce point.

      [ ] La recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration chargeé de la recherche internationale (règle 23.1(b)).

   b. [ ] En ce qui concerne **la ou les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale, (le cas échéant), voir le cadre n° 1.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre n° II).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre n° III).

4. En ce qui concerne le **titre**,
   [ ] le texte est approuvé tel qu'il a été remis par le déposant.
   [X] le texte a été établi par l'administration chargée de la recherche internationale et a la teneur suivante:

   PROCÉDÉ DE CONTRE-MESURE PAR MASQUAGE DE L'ACCUMULATEUR

5. En ce qui concerne **l'abrégé**,
   [X] le texte est approuvé tel qu'il a été remis par le déposant.
   [ ] le texte, reproduit dans le cadre n° IV, a été établi par l'administration chargée de la recherche internationale conformément à la règle 38.2(b). Le déposant peut présenter des observations à l'administration chargée de la recherche internationale dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. En ce qui concerne les **dessins**,
   a. La figure **des dessins** à publier avec l'abrégé est la figure n° _____
      [ ] proposée par le déposant.
      [ ] proposée par l'administration chargée de la recherche internationale, parce que le déposant n'a pas proposé de figure.
      [ ] proposée par l'administration chargée de la recherche internationale, parce que cette figure caractérise mieux l'invention.

   b. [ ] Aucune des figures n'est publiée avec l'abrégé.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/051144

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G06F7/72

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	LIARDET P-Y ET AL: "PREVENTING SPA/DPA IN ECC SYSTEMS USING THE JACOBI FORM" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS. 3RD INTERNATIONAL WORKSHOP, CHES 2001, PARIS, FRANCCE, MAY 14 - 16, 2001 PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE, BERLIN : SPRINGER, DE, vol. VOL. 2162, 14 mai 2001 (2001-05-14), pages 391-401, XP001061177 ISBN: 3-540-42521-7	1,2,12
Y	page 392, ligne 5 - ligne 13 page 393, ligne 1 - ligne 6 page 399, ligne 6 - ligne 12	8-11

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
11 février 2005	

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Verhoof, P

2

Formulaire PCT/ISA/210 (deuxième feuille) (Janvier 2004)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/EP2004/051144

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	TRICHINA E ET AL: "IMPLEMENTATION OF ELLIPTIC CURVE CRYPTOGRAPHY WITH BUILT-IN COUNTER MEASURES AGAINST SIDE CHANNEL ATTACKS" CRYPTOGRAPHIC HARDWARE AND EMBEDDED SYSTEMS - CHES 2002. 4TH INTERNATIONAL WORKSHOP REVISED PAPERS, REDWOOD SHORES, CA, USA, 13-15 AUG. 2002, 13 août 2002 (2002-08-13), pages 98-113, XP001160524 BERLIN, GERMANY, SPRINGER VERLAG	1,2,12
Y	page 100, ligne 11 - ligne 15 * Algorithm 1 * page 105, ligne 5 - ligne 10	8-11
X	US 2003/079139 A1 (DREXLER HERMANN ET AL) 24 avril 2003 (2003-04-24) alinéa '0018! - alinéa '0020!	1,3-6,12
X	WO 02/088934 A (LIARDET PIERRE-YVAN ; ROMAIN FABRICE (FR); ST MICROELECTRONICS SA (FR)) 7 novembre 2002 (2002-11-07) page 3, ligne 1 - ligne 21; figure 2	1,3,4,12
Y	EP 1 296 224 A (HITACHI LTD) 26 mars 2003 (2003-03-26) alinéas '0057!, '0058!, '0066!, '0070!	8-11

2

Demande internationale n°
PCT/EP2004/051144

RAPPORT DE RECHERCHE INTERNATIONALE

Cadre II Observations – lorsqu'il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche (suite du point 2 de la première feuille)

Conformément à l'article 17.2)a), certaines revendications n'ont pas fait l'objet d'une recherche pour les motifs suivants:

1. ☐ Les revendications n[os]
se rapportent à un objet à l'égard duquel l'administration n'est pas tenue de procéder à la recherche, à savoir:

2. ☐ Les revendications n[os]
se rapportent à des parties de la demande internationale qui ne remplissent pas suffisamment les conditions prescrites pour qu'une recherche significative puisse être effectuée, en particulier:

3. ☐ Les revendications n[os]
sont des revendications dépendantes et ne sont pas rédigées conformément aux dispositions de la deuxième et de la troisième phrases de la règle 6.4.a).

Cadre III Observations – lorsqu'il y a absence d'unité de l'invention (suite du point 3 de la première feuille)

L'administration chargée de la recherche internationale a trouvé plusieurs inventions dans la demande internationale, à savoir:

voir feuille supplémentaire

As a result of the prior review under R. 40.2(e) PCT,
no additional fees are to be refunded.

1. ☒ Comme toutes les taxes additionnelles ont été payées dans les délais par le déposant, le présent rapport de recherche internationale porte sur toutes les revendications pouvant faire l'objet d'une recherche.

2. ☐ Comme toutes les recherches portant sur les revendications qui s'y prêtaient ont pu être effectuées sans effort particulier justifiant une taxe additionnelle, l'administration n'a sollicité le paiement d'aucune taxe de cette nature.

3. ☐ Comme une partie seulement des taxes additionnelles demandées a été payée dans les délais par le déposant, le présent rapport de recherche internationale ne porte que sur les revendications pour lesquelles les taxes ont été payées, à savoir les revendications n [os]

4. ☐ Aucune taxe additionnelle demandée n'a été payée dans les délais par le déposant. En conséquence, le présent rapport de recherche internationale ne porte que sur l'invention mentionnée en premier lieu dans les revendications; elle est couverte par les revendications n [os]

Remarque quant à la réserve

☒ Les taxes additionnelles étaient accompagnées d'une réserve de la part du déposant.

☐ Le paiement des taxes additionnelles n'était assorti d'aucune réserve.

SUITE DES RENSEIGNEMENTS INDIQUES SUR PCT/ISA/ 210

L'administration chargée de la recherche internationale a trouvé plusieurs (groupes d') inventions dans la demande internationale, à savoir:

1. revendications: 1,2,7-12

   Procédé sécurisé de mise à la puissance dans un groupe additive

   ---

2. revendications: 3-6

   Procédé sécurisé de mise à la puissance dans un groupe multiplicative

   ---

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande Internationale No
PCT/EP2004/051144

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2003079139 A1	24-04-2003	DE 19963407 A1	12-07-2001
		AU 3015101 A	09-07-2001
		CN 1415106 T	30-04-2003
		WO 0148706 A1	05-07-2001
		EP 1272984 A1	08-01-2003
		JP 2003525538 T	26-08-2003
		ZA 200204746 A	13-12-2003
WO 02088934 A	07-11-2002	FR 2824209 A1	31-10-2002
		EP 1399807 A1	24-03-2004
		WO 02088934 A1	07-11-2002
		JP 2004531762 T	14-10-2004
		US 2004179680 A1	16-09-2004
EP 1296224 A	26-03-2003	JP 2003098962 A	04-04-2003
		EP 1296224 A1	26-03-2003
		US 2003059042 A1	27-03-2003

TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS

Expéditeur : L'ADMINISTRATION CHARGEE DE LA RECHERCHE INTERNATIONALE

PCT

NOTIFICATION DE TRANSMISSION DU RAPPORT DE RECHERCHE INTERNATIONALE ET DE L'OPINION ÉCRITE DE L'ADMINISTRATION CHARGÉE DE LA RECHERCHE INTERNATIONALE OU DE LA DÉCLARATION
(règle 44.1 du PCT)

Destinataire
GEMPLUS
La Vigie - Dpt Brevets
A l'att. de BRUYERE, Pierre
BP 90
13705 La Ciotat cedex
FRANCE

Date d'expédition *(jour/mois/année)* 06/09/2005

Référence du dossier du déposant ou du mandataire
GEM 1511

POUR SUITE À DONNER
voir les paragraphes 1 et 4 ci-après

Demande internationale n°
PCT/EP2004/051144

Date du dépôt international *(jour/mois/année)* 17/06/2004

Déposant
GEMPLUS

1. [X] Il est notifié au déposant que le rapport de recherche internationale a été établi et lui est transmis ci-joint.

Dépôt de modifications et d'une déclaration selon l'article 19 :
Le déposant peut, s'il le souhaite, modifier les revendications de la demande internationale (voir la règle 46):

Quand? Le délai dans lequel les modifications doivent être déposées est de deux mois à compter de la date de transmission du rapport de recherche internationale.

Où? Directement auprès du Bureau international de l'OMPI, 34, chemin des Colombettes 1211 Genève 20, Suisse, n° de télécopieur: +41 22 740 14 35

Pour des instructions plus détaillées, voir les notes sur la feuille d'accompagnement.

2. [ ] Il est notifié au déposant qu'il ne sera pas établi de rapport de recherche internationale et la déclaration à cet effet, prévue à l'article 17.2)a), ainsi que l'opinion écrite de l'administration chargée de la recherche internationale sont transmises par le présent formulaire.

3. [ ] **En ce qui concerne la réserve** pouvant être formulée, conformément à la règle 40.2, à l'égard du paiement d'une ou de plusieurs taxes additionnelles, il est notifié au déposant que

[ ] la réserve ainsi que la décision y relative ont été transmises au Bureau international en même temps que la requête du déposant tendant à ce que le texte de la réserve et celui de la décision en question soient notifiés aux offices désignés.

[ ] la réserve n'a encore fait l'objet d'aucune décision; dès qu'une décision aura été prise, le déposant en sera avisé.

4. **Rappels**

Peu après l'expiration d'un délai de **18 mois** à compter de la date de priorité, la demande internationale sera publiée par le Bureau international. Si le déposant souhaite éviter ou différer la publication, il doit faire parvenir au Bureau international une déclaration de retrait de la demande internationale, ou de la revendication de priorité, conformément aux règles 90*bis*.1 et 90*bis*.3, respectivement, avant l'achèvement de la préparation technique de la publication internationale.

Le déposant a la possibilité de présenter des observations de manière informelle au Bureau international sur l'opinion écrite de l'administration chargée de la recherche internationale. Le Bureau international enverra aux offices désignés une copie de ces observations, à moins qu'un rapport d'examen préliminaire international ait été établi ou doive être établi. Ces observations seraient également mises à la disposition des tiers mais pas avant l'expiration d'un délai de 30 mois à compter de la date de priorité.

Dans un délai de **19 mois** à compter de la date de priorité, mais seulement en ce qui concerne certains offices désignés, le déposant doit présenter une demande d'examen préliminaire international s'il souhaite que l'ouverture de la phase nationale soit **reportée à 30 mois** à compter de la date de priorité (ou même au-delà dans certains offices); si tel n'est pas le cas, le déposant doit accomplir, dans un délai de **20 mois** à compter de la date de priorité, les démarches prescrites pour l'ouverture de la phase nationale auprès de ces offices désignés.

En ce qui concerne d'autres offices désignés, le délai de **30 mois** (ou plus) s'appliquera même si aucune demande d'examen préliminaire international n'est présentée dans le délai de 19 mois.

Voir l'annexe du formulaire PCT/IB/301 et, pour plus de précisions quant aux délais applicables, office par office, voir les chapitres nationaux dans le volume II du *Guide du déposant du PCT* et le site internet de l'OMPI.

Nom et adresse postale de l'administration chargée de la recherche internationale
Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL-2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé
Ahmed Soliman

(Voir les notes sur la feuille d'accompagnement)

NOTES RELATIVES AU FORMULAIRE PCT/ISA/220

Les présentes notes sont destinées à donner les instructions essentielles concernant le dépôt de modifications selon l'article 19. Les notes sont fondées sur les exigences du Traité de coopération en matière de brevets (PCT), du règlement d'exécution et des instructions administratives du PCT. En cas de di vergence entre les présentes notes et ces exigences, ce sont ces dernières qui priment. Pour de plus amples renseignements, on peut aussi consulter le *Guide du déposant du PCT*, qui est une publication de l'OMPI.

Dans les présentes notes, les termes "article", "règle" et "instruction" renvoient aux dispositions du traité, de son règlement d'exécution et des instructions administratives du PCT, respectivement.

INSTRUCTIONS CONCERNANT LES MODIFICATIONS SELON L'ARTICLE 19

Après réception du rapport de recherche internationale et de l'opinion écrite de l'administration chargée de la recherche internationale, le déposant a la possibilité de modifier une fois les revendications de la demande internationale. On notera cependant que, comme toutes les parties de la demande internationale (revendications, description et dessins) peuvent être modifiées au cours de la procédure d'examen préliminaire international, il n'est généralement pas nécessaire de déposer de modifications des revendications selon l'article 19 sauf, par exemple, au cas où le déposant souhaite que ces dernières soient publiées aux fins d'une protection provisoire ou a une autre raison de modifier les revendications avant la publication internationale. En outre, il convient de rappeler que l'obtention d'une protection provisoire n'est possible que dans certains États (voir les annexes B1 et B2 du volume I du *Guide du déposant du PCT*).

L'attention du déposant est attirée sur le fait que des modifications des revendications selon l'article 19 ne sont pas permises lorsque l'administration chargée de la recherche internationale a déclaré, conformément à l'article 17.2), qu'aucun rapport de recherche internationale ne sera établi (voir le paragraphe 296 du volume I du *Guide du déposant du PCT*).

Quelles parties de la demande internationale peuvent être modifiées?

Selon l'article 19, les revendications exclusivement.

Durant la phase internationale, les revendications peuvent aussi être modifiées (ou modifiées à nouveau) selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international. La description et les dessins ne peuvent être modifiées que selon l'article 34 auprès de l'administration chargée de l'examen préliminaire international.

Lors de l'ouverture de la phase nationale, toutes les parties de la demande internationale peuvent être modifiées selon l'article 28 ou, le cas échéant, selon l'article 41.

Quand? Dans un délai de deux mois à compter de la date de transmission du rapport de recherche internationale ou de 16 mois à compter de la date de priorité, selon l'échéance la plus tardive. Il convient cependant de noter que les modifications seront réputées avoir été reçues en temps voulu si elles parviennent au Bureau international après l'expiration du délai applicable mais avant l'achèvement de la préparation technique de la publication internationale (règle 46.1).

Où ne pas déposer les modifications?

Les modifications ne peuvent être déposées qu'auprès du Bureau international; elles ne peuvent être déposées ni auprès de l'office récepteur ni auprès de l'administration chargée de la recherche internationale (règle 46.2).

Lorsqu'une demande d'examen préliminaire international a été/est déposée, voir plus loin.

Comment? Soit en supprimant entièrement une ou plusieurs revendications, soit en ajoutant une ou plusieurs revendications nouvelles ou encore en modifiant le texte d'une ou de plusieurs des revendications telles que déposées.

Une feuille de remplacement doit être remise pour chaque feuille des revendications qui, en raison d'une ou de plusieurs modifications, diffère de la feuille initialement déposée.

Toutes les revendications figurant sur une feuille de remplacement doivent être numérotées en chiffres arabes. Si une revendication est supprimée, il n'est pas obligatoire de renuméroter les autres revendications. Chaque fois que des revendications sont renumérotées, elles doivent l'être de façon continue (instruction 205.b)).

Les modifications doivent être effectuées dans la langue dans laquelle la demande internationale est publiée.

Quels documents doivent/peuvent accompagner les modifications?

Lettre (instruction 205.b)):

Les modifications doivent être accompagnées d'une lettre.

La lettre ne sera pas publiée avec la demande internationale et les revendications modifiées. Elle ne doit pas être confondue avec la "déclaration selon l'article 19.1)" (voir plus loin sous "Déclaration selon l'article 19.1)").

La lettre doit être rédigée en anglais ou en français, au choix du déposant. Cependant, si la langue de la demande internationale est l'anglais, la lettre doit être rédigée en anglais; si la langue de la demande internationale est le français, la lettre doit être rédigée en français.